AD-A070 176 NAVAL POSTGRADUATE SCHOOL MONTEREY CA F/G 9/2
SECURITY/PRIVACY CONSIDERATIONS IN DATA PROCESSING.(U)
MAR 79 K L NELMS

UNCLASSIFIED NL

| OF |
AD
A070176

END
DATE
FILMED
7-79
DDC

NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

SECURITY/PRIVACY CONSIDERATIONS
IN DATA PROCESSING

by

Kenneth Lee Nelms

March 1979

Thesis Advisor: J. W. Creighton

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) SECURITY/PRIVACY CONSIDERATIONS IN DATA PROCESSING		5. TYPE OF REPORT & PERIOD COVERED MASTER'S THESIS, MARCH 1979
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) KENNETH LEE NELMS		8. CONTRACT OR GRANT NUMBER(s) 12 94p.
9. PERFORMING ORGANIZATION NAME AND ADDRESS NAVAL POSTGRADUATE SCHOOL MONTEREY, CA 93940		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS NAVAL POSTGRADUATE SCHOOL MONTEREY, CA 93940		12. REPORT DATE MARCH 1979
		13. NUMBER OF PAGES 94
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Computer Security
Computer Privacy

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This thesis contains the result of a study of the computer security/privacy problem. The primary purpose is to present the fundamental issues of computer security in survey form. Various protection schemes and administrative techniques are examined and related to security programs. Problems in the development of secure systems for the future are appreciated, and approaches for secure interim programs are suggested. This paper is directed at data processing managers with the goal of helping them better understand

DD FORM 1473 1 JAN 73 EDITION OF 1 NOV 65 IS OBSOLETE
(Page 1) S/N 0102-014-6601

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

251 450 79 06 20 075 JOB

the vulnerability of data in computers. It is intended to foster a sense of security awareness among people who use computers to process data.

Accession For	
NTIS GRA&I	
DDC TAB	
Unannounced	
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or special
A	

DD Form 1473
1 Jan 73
S/N 0102-014-6601

Approved for public release; distribution unlimited

SECURITY/PRIVACY CONSIDERATIONS IN DATA PROCESSING

by

Kenneth Lee Nelms
Lieutenant, United States Navy
B.A., University of Guam 1969

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN TELECOMMUNICATIONS SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1979

Author Kenneth Lee Nelms

Approved by: D W Creighton
Thesis Advisor

Robert S. McComas
Second Reader

Chairman, Dept. of Administrative Sciences Department

[illegible]
Dean of Information & Policy Sciences

ABSTRACT

This thesis contains the result of a study of the computer security/privacy problem. The primary purpose is to present the fundamental issues of computer security in survey form. Various protection schemes and administrative techniques are examined and related to security programs. Problems in the development of secure systems for the future are appreciated, and approaches for secure interim programs are suggested. This paper is directed at data processing managers with the goal of helping them better understand the vulnerability of data in computers. It is intended to foster a sense of security awareness among people who use computers to process data.

TABLE OF CONTENTS

I. INTRODUCTION

Managers are becoming increasingly concerned with issues of computer security and privacy. There is growing awareness among computer users of the vulnerability of their data and the potential cost of its loss. Managers are now aware that information is a unique asset that can be stolen even though it may never be missed. [Ref. 10] The computer has provided for industrial growth and new applications to the extent that the majority of large organizations can now only function for a matter of a few hours without the proper functioning of their computer. The computer has made it possible to store, retrive, and to manipulate data to an extent not thought possible a few years ago. This has increased the scope of data processing applications into new areas. This increased scope has brought with it increased security problems. We must now come to grips with the security problem and find a solution through common sense management and further research in hardware and software applications.

Security involves the hardware manufacturer, the software developer, and user; and encompasses physical facilities and operational procedures, as well as programming techniques. [Ref. 16] Computer security requires the protection of system associated physical assets, facilities, and processed data and programs. It involves the protection of data against accidental or intentional disclosure to unauthorized persons,

or unauthorized modifications or destruction. Of particular interest are the data processing hardware, software, people, storage media, input/output areas, communications terminals and transmission paths.

System security was neglected in early designs and development of computers. Initially the prime objectives of system manufacturers was to make it work and to find new applications. As computer usage expanded into government and industry, it soon became obvious that adequate protection was not provided for processed data. Federal laws requiring the protection of national security information were strengthened and new laws were passed to protect the privacy of individuals. Economic considerations and common sense soon dictated that industry join government in demanding more secure systems.

The U. S. Government is now spending over $10 billion annually for the operation of computer-based information systems. [Ref. 9] Public interest has the right to expect government to do everything possible to maximize economy and manage the information systems effectively from a security/privacy point of view. Yet, top management has failed to exercise leadership to focus information technology applications toward attainment of specific objectives. Specifically there has been no policy guidance on the need for detailed program analysis and program operation. For these reasons much of the potential power of information technology still remains at a primitive level of application.

Federal, state, and local governments are proposing and passing security and privacy legislation. The new laws restrict the manner in which information about individuals can be collected, stored, and disseminated. In addition, much of this legislation dictates that certain security safeguards be implemented by the computer user. For example, national laws now apply not only to paper in filing cabinets, but also to data in the computer.

The vulnerability and increased use of computer systems has led to an increasing number of security incidents. The failures that have always resulted in security problems in manual data systems are the ones present in automatic data processing systems: errors, omissions, floods, fires, explosions, frauds, thefts, extortions, vandalisms, larceny, expionage, and compromises of personal rights.

The problem of security of information has been with the world since the first bit of information was processed. Stored or transmitted information has been subject to destruction by natural disasters and interception by man from the beginning. The computer has only made it possible to manipulate larger amounts of data and in that way it has expanded and compounded the security problem. Certainly, the invention of the computer has led to a serious problem for the public, a threat to their security and privacy. In his book, Future Shock, Alvan Toffler says, "we have scarcely touched on the computer revolution and the far-remifying changes that must follow in its churning wake". [Ref. 45]

A. OBJECTIVES

The objectives of this thesis are to present the main issues of computer security and to enhance an appreciation of the problems involved. The fundamental elements of computer security problems applicatable to both government and private business will be examined. This is a study of computer security problems confronting the data processing manager. It is intended to impress upon the reader the seriousness of the computer security problem in hopes of preventing future security violations. This paper is not intended to be technical or to describe all of the protection schemes which have been proposed and/or implemented, but to describe the data processing security situation.

Of particular interest to computer security is the impact of the Privacy Act of 1974. Computer security has only recently been recognized as a major problem in data processing, and security considerations have seriously lagged behind technical developments. Much work remains before the level of security in data processing is improved to an acceptable level under current laws. Part of the computer security problem is technical in nature, i.e. cryptology and system design, but the major portion of the problem is administrative. Proper system design and the use of cryptology will minimize the necessary administrative controls, but future technical innovation alone will not resolve the problem no more than past technical advances have lessoned the administrative burden. Basically, computer security will remain an administrative/educational problem. [Ref. 50]

Therefore, management must be ready to look at computer security in a comprehensive manner. Data processing managers must understand the vulnerability of data that is stored in computer systems. Hopefully, this thesis will make a contribution toward that goal. Methods of protecting data are more varied than data processing systems: however, some methods of protecting against accidental or deliberate loss are just common sense. Based on the premise that the best way to begin preventing computer abuses is to understand how they happen, typical computer crimes are examined.

Primary concerns are to understand the problem, examine approaches toward development of a secure system, suggest methods of providing protection by a security program, and appreciating planning and development problems.

A secondary objective of this thesis is to provide the basis for a follow-on thesis in the form of a training film. The envisioned film would be designed to foster a sense of security awareness among military data processing managers and supervisors.

B. SCOPE

It is recognized that the scope of this thesis is quite wide. Either of the primary chapters could have served as an adequate subject by itself for thesis research. However, from a security managment point of view, an effective data processing security program cannot be built on just physical security or cryptology alone. An effective data processing security program will require a unique mix of all the subject

areas covered in this thesis. Each program must be tailored to the specific needs and requirements of the organization for which it is designed.

To understand the problem, it is necessary to be aware of the information presented in the chapter on computer crimes and abuses. A manager must know the problem before he can provide a solution.

The chapter on privacy leaves little doubt as to the seriousness of the problem. The legal and social implication of data processing security/privacy simply must be understood by anyone in charge of a computer facility today. Current laws place the ethical and legal responsibility for security clearly with the data processing manager. The rapid expansion of the use of computers via the distributed processing concept compounds the data processing manager's security problem. He must call upon a wide variety of administrative and technical skills to manage a balanced and comprehensive security program. For this reason, it is necessary to include chapters on both technical and administrative procedures.

The scope of the problem today is too wide to be delt with by just personnel and physical security procedures, and a security program built solely on technical application cannot be effective. The manager involved with data processing today must understand all the technical and administrative implications of electromagnetic phenomena, software, personnel and cryptology. He must know how to manage by such techniques as risk analysis and he must also know when and how to audit or buy insurance.

II. COMPUTER CRIME AND ABUSES

In the United States between one and two billion dollars a year is lost because of employee theft of goods, and another three billion is lost by embezzlement. An additional five million is lost to industrial espionage, and much more is lost to information thievery. No one knows how many cases of computer abuse and invasion of privacy and confidentiality have been perpetrated, but Anderson and Company, a CPA firm, estimates that losses from computer crime will exceed 2 billion dollars per year by 1982. [Ref. 37] Known computer-related fraud losses in 1974 amounted to $200 million and it has been estimated that this represents only 15% of the actual fraud which occurred during that year. Commercial banks alone handle over 100 million transactions each business day. These transactions involve 100 million separate accounts in over 14,000 institutions and are of the order to $120 billion.

A. THE COMPUTER CRIMINAL

The Stanford Research Institute indicates that 66% of the total human threat to computer installations is comprised of data processing personnel employed by the victim organization. Research has also produced the individual profile: [Ref. 41]

1. Highly skilled
2. 18-30 year old male
3. Bright, eager, and highly motivated

4. Exhibits the Robin Hood Syndrome

5. Enjoys his work

6. University trained

7. Great fear of detection and exposure

A clever programmer can introduce into a coded procedure subtle changes that lie hidden and dormant, perhaps for months; these changes are then triggered by an external event, such as the disappearance of the programmer's name from the payroll.

The more skillful and knowledgeable the person, the more dangerous he becomes if his actions and intent are directed against the organization. One should assume the potential attacker will know as much about the system and its security features as its designers. For someone skilled in the art, penetrating an operating system takes little more effort than solving a difficult crossword puzzle, and it can be considerably more lucrative. Computerized larceny has several advantages over regular old style larceny. Computerized larceny is seldom discovered and is difficult to prosecute when it is discovered. Computer criminals are seldom professional criminals, but they are usually much more successful. They obtain much more money than other criminals and are selcom caught.

B. SOME FACTS AND STATISTICS

Much of our knowledge is based on the findings of a Stanford Research Study of 129 computer related incidents of loss, injury, or damage. /Ref. 36/ Of these, 24 involved vandalism, 41 information or property theft, 43 financial fraud or theft,

and 21 unauthorized use or sale of services. Incidents ranged from stealing flowcharts from waste baskets, to penetration of the operating system for purposes of industrial espionage. In two cases computers were actually shot with pistols. It can be concluded from the study that security measures within a computer system at the present stage of development can be only as effective as the physical and personnel security surrounding the system.

Embezzlements with the aid of computers are for approximately ten times larger amounts than without the aide of computers. Theft of property with the aide of computers has also been much higher in value than without the assistance of computers.

C. A SURVEY OF COMPUTER CRIMES

The most recent publicized computer crime involved the theft of $10.2 million in bank funds. A computer consultant working alone transferred the money from San Diego via New York to Switzerland and on to a Soviet diamond compnay. The money was used to buy $13 million worth of diamonds. Fortunately for the bank, the diamonds were recovered and became bank property, and the bank made a tidy $3 million profit.

The first programmer convicted for stealing programs was in 1964 and he received a sentence of five years imprisonment for apparently turning over his employer's proprietary computer program to an outsider. The first federal computer criminal case occurred in 1966 when a 21 year old programmer put a patch on the demand deposit accounting program he

developed to make it ignore overdrafts on his own checking account.

Some typical computer crimes and abuses follow:

1. An employee of the Encyclopedia Britannica was able to walk off with a tape in his briefcase, containing a customer list. He used a service bureau to duplicate the list for sale.

2. An antiwar group destroyed data processing media using magnets, reconstruction costs were $100,000.

3. An Army data center was bombed by dissidents causing $1.5 million damage, loss of one researcher and a 20 year data base. /Ref. 4/

4. A disgruntled Army officer awaiting retirement erased purchasing data from magnetic tape.

5. A Department of Defense executive bribed a Pentagon data processing employee to do computer work for a foreign interest.

6. Hidden wireless transmitters were found inside a computer processor unit in a U. S. security agency office.

7. Typical of the threat of privacy breaches in data security is the case of a G. I. who had just returned from the Vietnamese war and was offered $10,000 by organized crime to become a contract killer. /Ref. 48/ Someone had gotton hold of his army record and found that he had been involved in several "kills" in Viet Nam. Similar problems exist throughout the data field where information is compiled on individuals.

The foregoing are only examples of an infinite number of ways the computer system can be abused. As illustrated by the examples, most criminal uses of computers are by individuals, but organized crime has not overlooked the possibility of large easy profits through the use of computerized embezzlement. In 1968, a Diners' Club credit card company lost over $1,000,000 in a credit card fraud. A computer printout of real Diners' Club customers was used to make phony credit cards; when discovered over 3,000 cards had been used for the safe 30-day period before the real customers complained about their bills. This was traced to an interstate crime organization in New York and Florida.

D. CAUSES OF COMPUTER CRIME

Computer crime cases investigated or reported show some causes worthy of highlighting. Crimes and abuses in the data security area show the following five general conditions that allowed the crimes to take place.

1. Almost all of the crimes and abuses studied could have been prevented with better manual procedures and internal controls.

2. Most computer crimes or abuses were discovered by accident.

3. The cost of crimes involving computer systems appeared to run much higher than in those involving manual systems.

4. Most computer crimes are not reported and, therefore, very little is known about the true extent of computer crimes and abuses.

5. Audit trails through a computer process are generally lacking; it is possible to steal one's way to fortune, using a computer to extract nickels and dimes from many accounts, the differences being unoticeable to the individuals affected.

Several criteria indicate that the climate for computer crime is good but becoming better. Some companies even fail to use an independent audit and computer installations have a tendency to cause more and more of the checking and balancing to be done within the computer department itself. Physical handling of assets, recording of transactions, and supervision are actions which should be independent of each other. Embezzlement often occurs because one individual has complete authority over an asset with no checks. Dual control or simply rotation of duties will minimize the opportunities in many cases. [Ref. 40]

If better protection measures for computer information are not developed, past computer crimes will be minor in comparison to new crimes that are likely to take place. The future looks good for a criminal who specializes in manipulating or stealing computer information or the ameteur who wants to start out in this field.

III. THE PRIVACY ISSUE

Privacy is the right of individuals to control the collection, use and dissemination of personal identifiable information: to determine what information about themselves is made available to whom and to what extent. In another context, the meaning of privacy is the right to be left alone.

The threat to the individual is loss of anonymity, fear of minor exposure, and fear of de-personalization of social values. The fear of erroneous treatment, the fear of unfair treatment and the fear of hostile treatment are all part of the computer/privacy problem.

There is an atmosphere in both industry and government today that seems to exist in which the individual in exchange for benefit or service is assumed to waive all interest and control over the information collection, storage, and dissemination. From privileged files, such as retirement records, or financial records, some users compile mailing lists to sell, or even sell proprietary data to competing contractors, and personnel information may be stolen for illegal purposes such as blackmail.

Potentially the Social Security Number could become a standard universal identifier of American citizens. It could be used to track all the errors, omissions, and/or sins of an individual from cradle to grave. [Ref. 48] The record keepers in the federal government already know more about us than we

know about ourselves. The list is enormous as indicated by Bottlieb and Borodin in their book, Social Issues in Computing. [Ref. 12]

Their list of the following types of data commonly gathered about individuals is indicative of the privacy threat from computer listings.

1. Identification:

Name, maiden name (if applicable), social insurance number, date of birth, place of birth, citizenship, address, appearance, physical features, marital status, names of family.

2. Employment:

Occupation, current employer, employment history, earnings, education and training, qualifications.

3. Medical:

Current health, medical description and history, genetic factors, reportable diseases, x-rays, immunizations, dental history, health plan and participation.

4. Education:

Schools attended, educational attainments, professional licenses, awards, loans.

5. Taxation:

Earnings, investment income, foreign holdings, dependents.

6. Financial:

Bank account history, holdings, earnings, credit and load history, life insurance.

7. Military Service:

Rank and qualifications, service record, disciplinary record, medical record.

8. Vehicle registration:

Owner, property identification, description, zoning, assessment and taxation, uses.

9. License and permits:

Identification, type of license, dates, insurance.

10. Travel:

Passport, visas, countries visited, customs and duty payments.

11. Welfare:

Agency, history, dependents, aid received, earnings.

12. Civil action:

History, court identification, dates, outcomes.

13. Police records:

Offenses, warrants, convictions, confinements, probation and parole, political affiliations.

14. Customer accounts:

Company, sales history, credit status.

15. Life Insurance:

Idenfication, value, history, other insurance, medical data.

16. Mailing lists:

Type, source, customer profile, history of purchases.

17. Biographical:

Identification, curriculum vitae, accomplishments,

publications, memberships, relatives.

18. Membership:

Organization, history, participation, financial, relatives.

Record keeping has gone on since the Stone Age [Ref. 48] but record keeping techniques have grown to keep pace with the sophisticated ways of data gathering, and the incessantly increasing demand for data. The Federal Government has at least twenty-seven agencies and bureaus gathering information, much of which is quite private and personal. [Ref. 16] In June of 1974, the results of a study by the staff of the Senate Judiciary Subcommittee on Constitutional Rights was released. [Ref. 20] This study showed the scope of the federal government's collection of personal data on individuals: "the study found 858 data banks in 54 federal agencies, the majority of them not legislatively authorized".

A. LEGAL BASIS OF THE RIGHT TO PRIVACY

The proliferation of information systems containing personally identifiable information has made it necessary to pass statutory laws in the United States to protect the privacy of individuals. The issue of computers and privacy first came to a head in 1966 when the Federal Bureau of the Budget proposed a Federal Data Center. The public and congress saw this as a central file of dossiers, too centralized and too accessible. The government would have a much too powerful tool for controlling its subjects. The idea was dropped. In 1969 Congress passed the Fair Credit Reporting Act. This act was

clearly aimed at the credit bureau's ability to produce a dossier on all the citizens in the United States. The fear of a "suffocating sense of surveillance", and a growing distrust of too much government are both natural concommitants of computer data banks.

The concept of personal privacy and individual rights is really as old and as basic as our Bill of Rights. Most Americans accept it as the bedrock of their freedom and give it little concern. That is, until they find how insidiously their privacy is being invaded or their rights ignored. The constitution of the United States doesn't mention a right to privacy explicitely, only three state constitutions do: Alaska, California and South Carolina. However, personal privacy derives some protection from judicial interpretation of some provisions of the Bill of Rights.

In the law history of the United States, privacy had its beginning in approximately 1890 in a Law Review published by Louis D. Brandeis, later to become a Justice of the Supreme Court. [Ref. 16] He developed the history of the Right of Privacy and strongly suggested the direction of its application. [Ref. 1] In Griswold vs. Connecticut (1965), the Supreme Court clearly indicated that the Ninth Amendment contained the right to privacy. The Ninth Amendment provides that "the enumeration of the Constitution of certain rights shall not be construed to deny or disparage others retained by the people". The Supreme Court held that one of those rights not mentioned in the Bill of Rights and which was

retained by the people was the right to privacy.

The concept of privacy has its origin in early English common law cases which provided that individuals had a certain right not to have facts about their personal life publicized. The original cases involved excesses of the press in publishing information about individuals which caused an unjustifiable infliction of mental pain and distress.

B. THE PRIVACY ACT

"Records, Computers and the Rights of Citizens", a report prepared for the Department of Health, Education and Welfare, and published in July 1973, gave impetus to the current concern over infringement on individual privacy caused by the leaking of personal data, which in turn gave impetus to the passage of the Privacy Act of 1974. Although the Privacy Act was aimed primarily at federal agencies, it established a Privacy Protection Study commission which can affect the private sector. In any event the Privacy Act, (Public Law 93-579), Section 552a lists certain responsibilities management must fulfill. In short, the first responsibility is to determine if a system of records are covered under the Privacy Act. If so, applicable protection requirements must be met.

The Primary purpose of the Act was to lay down specific guidelines for all federal offices which keep information or files on any individual. /Ref. 20/ Generally the Act protects individuals against information handling practices that may cause harm or embarrassment. The Act provides for a $5,000 fine for anyone not complying with the provisions of

the Act, and also allows anyone harmed to sue the person who violates the Act.

Public Law 93-579 amends Chapter 5 of Title 5 of the United States Code. It applies to United States Federal Government Agencies and private contractors who are performing a record-keeping service for a Federal Agency.

Public Law 93-579 created a set of standards for the collection, maintenance, use and dissemination of personal information in both manual and automated systems. A Code of Fair Information Practices are incorporated into the Privacy Act. The basic principles are abbreviated below:

1. There must be no personal data record-keeping system whose very existence is secret.

2. There must be a way for an individual to find out what information about him is in a record and how it is used.

3. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for another purpose without his consent.

4. There must be a way for an individual to correct or amend a record of identifiable information about him.

5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for thier intended use and must take precautions to prevent misuse of the data.

These principles incorporated in the Privacy Act (Section 552b) permit exceptions when "determined by specific statutory

authority". Legislating the right to privacy must be balanced against equally valid public interests in freedom of information, national defense, foreign policy and law enforcement.

The technical problem of protecting data in a computer system is the same whether national security or personal privacy is involved. In the Navy we must be concerned with both problems. Automated medical systems fall strictly under the Privacy Act, automatic command and control systems ususally do not involve privacy but often require protection of nationally classified information. Intelligence systems may involve both security and privacy protection. The Navy is required to satisfy the Congress that certain considerations have been met with respect to the Privacy Act for all systems. This responsibility lies strictly with data processing management. Central to the privacy issue is computer security, for privacy can be guaranteed only if computer security is complete. Without computer security, promises of privacy can be easily violated.

C. THE PRIVACY PROBLEM IN PERSPECTIVE

Key information issues identified by the Domestic Council Committee on the Right of Privacy identifies at least a dozen major considerations: /Ref. 25/

1. the true needs of information
2. inter-agency information sharing
3. freedom on information
4. information as property
5. industry and government competition
6. privacy

7. federal policy laws

8. rational information policy and legislation

9. government R&D for information

10. trans-border information flow

11. technology transfer by information

12. media technology

These key issues only begin to describe the complexity of the data processing world where interwoven action in one area impacts all or most of the others. National policy must be strong enough to answer questions such as who will control electronic mail, electronic funds transfer, telecommunications, freedom of information, privacy as well as other issues. If not, the results will be inefficient, ineffective, and most likely catastrophic.

The complete fear associated with the privacy problem was eloquently summed up by the statement by Justice Brandeis in the 1928 case of Olmstead versus the United States: /Ref. 48/

> "Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning, but without understanding."

IV. THE DISTRIBUTED PROCESSING PROBLEM

The concept of distributed processing systems is rapidly gaining universal acceptance; however, it is not clearly understood. A standard definition of distributed processing has not yet gained wide acceptance. Current literature contains numerous examples of interchanging the concepts of "network" and "distributed processing systems". Even in context, it is difficult to discern exactly which phrase is the proper choice.

Because of the anticipated future significance of distributed processing, two workshops were conducted at Brown University during 1976 and 1977. The conferences were convened to develop insight into the implications of distributed processing, and to attempt to define the term itself. The conferences proposed a definition that includes five separate facets:

1. A multiplicity of general purpose components that can be dynamically assigned specific tasks.

2. A physical distribution of the physical and logical components using a communications network.

3. A high-level operating system that integrates and controls all of the distributed components.

4. System transparency, meaning that a user can request and receive a service without knowing or caring from where the service is being provided.

5. Cooperative autonomy, meaning essentially that

processors in the distributed system cooperate on a co-equal protocol basis. The general opinion formed during the aforementioned converences was that a distributed system has all five features, yet only the communications subsystem of the ARPANET presently meets all of the criteria.

The design and implementation of a security program for a distributed processing system is a data processing manager's nightmare. Security in a distributed system can only be as strong as the security at every node in the system, a breach of security at one site can conceivably impact upon one or more other sites in the system. Achieving security in computer networks is a far greater challenge than achieving it in stand-alone systems. Security in a distributed system demands all the considerations given to security in a centralized system, plus many additional considerations.

Remote terminals and multiple processors are the single greatest problems and complicating factor in data processing security. Remote access to computers has resulted in an expanded user population and terminals which are placed in locations potentially more hostile than the host environment. Lack of administrative and operational controls over users at the remote access terminals have accelerated this problem. On-line or real time systems present special security problems. People interact with the programs and the memories faster, data is available faster than in batch oriented systems, data is up to date, and data can be altered quickly.

The following list exemplifies leakage or loss unique to

remote computing:

1. Physical access to the computer cannot be isolated to the environs of a machine room, thus complicating the physical security problem.

2. The communications lines are vulnerable to tapping or passive monitoring of emanations. Crosstalk between communications lines or within the switching centrals can present a vulnerability.

3. In a networked system, a large population of users with varying needs to know will be interacting simultaneously with the system.

4. The more extensive the network, the greater the probability of system error and vulnerability to intrusion.

5. It is impossible to verify that any large software system is completely free of errors and anomalies.

6. The remote location of a terminal introduces the problem of identification of the user of the system.

An interesting twist to the identification problem is the requirement to have the computer properly identify itself to the user. The potential need for such a scheme is best explained by the following situation. Several computer science students wrote a program to simulate the normal log-in procedure on a terminal. They left the terminal running, executing the program. Prospective users would log in and authenticate to the program, which filed that information. The program would then simulate a system crash. That forces the users to log back into the system, this time actually gaining access

to the computer resources. In that manner, the students obtained 100 user log-in precedures. The implications of this sort of masquerade are obvious and illustrate the potential requirement to have the computer identify itself to the satisfaction of the user.

Abuses of on-line systems can be relatively easy for a system not designed from the ground up to provide security. For example, a large oil company's inspection of usage logs revealed an unusually high rate of access to certain files for which normal user's would have no need. Further investigations revealed an ex-employee, in possession of all the correct passwords, was using his own terminal at home to dial through the public phone system and drain off company financial data. His motive was to gain inside financial information for playing the stock market. There are various schemes to limit the effectiveness of intruders. One such scheme was just demonstrated, i.e. the user log. Each user is periodically provided information on his usage. If he did not in fact use the system on all those occasions, his identity and authentication have been compromised and must be changed.

A promising approach to access control is to use a minicomputer as a means of authenticating and controlling access to the system or its resources. The physical separation and smaller operating system in the minicomputer would enhance security because it would be easier to check for tampering and it would be easier to control The employment of specialized front-end processors for handling communication is desireable.

It would be questionable practice to tie up large computers for this and such tasks as encryption, decryption, and sending and receiving.

One of the most complex problems that must be faced in the design and implementation of distributed processing systems is the problem of providing security for data in transmission. All technical resources will be strained to assure security over communication lines. The threat is the "bugging" of the communication line and node linkages which are extremely vulnerable to attack. Messages going across lines can be read, copied, altered, and duplicated. The equipment needed for this infiltration is readily obtainable from any radio parts supplier at little cost. Fortunately, this intrusion method can be effectively countered by a high level encryption system as explained in Chapter IX.

Once a communications line leaves a particular facility, it is joined by scores, or even hundreds or thousands, of unmarked lines. The transmission may even be multiplexed and sent via microwave. The point is that wire-tapping or interception of data can be difficult after the transmission line leaves the immediate area. Therefore, wire-tapping is most likely to occur within the building housing either the terminals or the receiving computer. The connection boxes at those locations must be secured.

The first step toward achieving any kind of security in a resource shared system is to apply those principles of protection that would normally be used in a local or one node system.

If the basic principles of physical and administrative security, as well as adequate audit trails and backup are followed, then the necessary groundwork will have been laid for implementation of protection throughout the network.

Good security procedures are a viable philosophy that must permeate all activities in managing data, hardware and software. The concept of establishing and nurturing that positive philosophy will go even farther in a distributed system. The integration of geographically dispersed computer systems implies the need for the concomitant requirements for data encryption and stringent access controls for all the system resources.

V. PHYSICAL SECURITY

Physical security is the most basic part of the security program. Classified information on a computer must be protected just like classified information in more traditional forms. However, the problems in protecting data in a computer system are more subtle and more complex and cannot be solved completely by a massive dose of cryptography. We also must protect the computer systems as well as the data if we are to prevent alteration, destruction or loss by sabotage and espionage.

Problems in physical computer security are complicated by the remote location of terminals, the increased amount of resource, and the presence of distributed intelligence, and distributed data banks. All computer installations should be a restricted area even if they don't deal with sensitive information. Restricted access will serve as the front line of defense. Structural integrity of the facility is an important ingredient, not only for the hardware but for the libraries as well. A less obvious safeguard is simply not to have large signs proclaiming the location of the facility. However, the factors of physical security such as site selection, fire and damage control and access control will likely be delt with long before the data processing manager arrives on the scene.

A. HARDWARE FAILURES

To prevent hardware failures, it will be necessary to maintain a high level of hardware maintenance. A thorough and regularly scheduled maintenance program should be designed to keep hardware in top operating condition. Hardware failure can cause serious losses to valuable data. For example, serious damage to files can result from any device mishandling magnetic storage media such as tapes, disks, or drums. The read/write heads on these devices should not physically touch the media. If the head does touch the media, the surface of the media, and of course the data contained thereon, will be damaged along with the read/write head itself. Such an occurrence is known as a head crash. Strict adherence to good handling procedures and cleanliness can do much to prevent such occurrences. The tolerances of the devices are so fine that fingerprints and even small particles of dust or smoke can cause damage to read/write heads and storage media.

1. Back-up Files/Hardware

Minimizing damage due to a hardware of software failure can generally be accomplished by a back-up file. The concept of retaining "father" and even "grandfather" files is a widely accepted practice in data processing. Back-up processors which are able to process in a degraded environment minimizes the impact of a hardware failure. An organization's efforts directed toward minimizing damage due to hardware or software failure can generally enhance the recovery from such a failure. As in so many cases, back-up capability in hardware and files is a key factor.

B. NATURAL DISASTERS

Acts of God include such threats as fire, flood, severe weather, earthquakes and acts of war. Aside from fire protection, there is not a great deal that an organization can do to prevent the occurrence of such destructive acts of God. [Ref. 55] An organization which is dependent on its computer system can suffer a large financial loss and degraded capability if that system is damaged or destroyed by intentional sabotage or natural disaster. The publicity attendent on bombings of computer installations has alerted many managers to that potential danger. But fire, earthquakes, or hurricanes can be almost or even more damaging and may be more likely to occur. These things need to be evaluated and taken into account when planning a security program.

Probably the biggest threat universally faced by computer facilities is fire. A Pentagon fire in the early 1960's destroyed $6.7 million worth of equipment and over 7,000 reels of magnetic tape. A fire does not have to be in the machine room to completely cripple the data processing operation. Fire can deny air conditioning, or cause smoke damage if in an adjacent space. Floods and natural disasters also should be considered when planning the recovery phase.

1. Recovery Plan

Too few systems have a usable disaster recovery procedure in the event of major destruction or sabotage. In order to move quickly and efficiently into emergency operations, the back-up recovery plan should be prepared, published

and rehearsed. The plan should be stored off-site. It should contain an inventory of items essential to recovery, a list of alternate resources of supply, and people to contact at the supplier. The plan should be simple and flexible. It is more important that the plan identify alternatives than give detailed instruction. A written mutual assistance agreement should be negotiated with a compatable installation. This agreement should identify the amount of computer time to be made available to a recipient as well as specifying the time of day during which the time will be provided. This mutual assistance agreement should be stored with the back-up/recovery plan.

2. Redundancy

Recovery from damage due to acts of God can also be greatly enhanced by reasonable redundance. Duplicate files maintained on tapes or other magnetic media (or even cards) should be stored with some separation from the main library. Duplication would serve no purpose if one fire or flood would destroy both the original file and the duplicate at the same time. In considering duplication of extensive file systems, the cost of such duplication must be weighed against both the value of the data and the probability of destruction.

C. CONTROL OF DOCUMENTATION

Control of documentation is a major area of the overall security program. Prevention of unauthorized copying is an important aspect of documentation control. If possible, paper which is resistant to photocopying equipment should be

used. A better approach would be to use tape or micro-film for the back-up copy. The program library must provide safe storage as well as distribution control. The back-up copy must be protected by the same measures used to protect the most sensitive file copied.

Back-up program copies must be stored in vaults or fire resistant cabinets. Copies must be updated regularly. Two copies are best, one for immediate use in the installation and one at some safe remote storage location. Positive inventory and accounting procedures for both should be installed.

D. ACCESS CONTROL

If possible, personnel traffic should be limited to one entrance where security is provided by a cypher lock or guard/ badge checking system. All visitors should be escorted when in a restricted area and logged in and out in a visitors log. The entrance should be within view of the normal working area. How the installation is designed will influence how easy the controlled access problem will be.

E. SUPERVISING PHYSICAL SECURITY

Data processing managers should take an intense personal interest in daily informal observations. Make sure that bad practices are not allowed to get started, and make sure prescribed procedures are followed. Good physical security practices can be negated by the lack of adequate supervision. Be on the look out for such weaknessess as the company with cipher locks guarding all doors to its computer installation

and unlocked distribution boxes for the computer output in a public hallway, or worse yet unguarded access terminals. [Ref. 54] In one case a computer was used to steal more than a million dollars and the information needed to crack the system was found in a trash can in the street outside the company grounds.

VI. PERSONNEL SECURITY AND EDUCATION

Computer security must be viewed as a multi-dimensional problem. Personnel security is unfortunately linked with physical security in a manner that produces what has been labeled "the fox in the chicken coup" problem. When the machine room doors are locked, we are essentially locking in our personnel security problems since, in batch processing, the people that we have the most reason to fear are our own technical and operational personnel. [Ref. 48]

College students today are supplied with computer time and computer terminals for their academic pursuits. However, most of the time-sharing systems and many of the campus computers are unable to control the work submitted by a student on a legitimate job number. Most schools don't even attempt to control the work flowing through the center. [Ref. 54] Thus in addition to providing the students with an excellent education in computer science, the student prone to mischief or maliciousness has virtually free access to terminals and computer capability. This has all the makings of a first-class threat which follows none of the logic of economics, knows no business morals, and due to the vast leased communication networks and the availability of WATS lines, leaves no company truly immune. It is generally recognized that organized crime has the intelligence and the resources to penetrate almost anywhere they choose. The advanced college student presents

a similar threat. He has the intelligence, he has the time, he doesn't mind working strange schedules, he has access to terminals, to communications, to computers for decrypting, and, if his interest does not wane, he can put together a team sufficiently talented to constitute a major threat to most industrial systems.

Education plays a large part in developing secure systems of the future, if vulnerabilities are not identified solutions will not be developed. However, college students given large leeway in fiddling with computers are not necessarily learning the basics of computer operations in the way that we would prefer.

Donn Parker, the nations leading expert on computer crime, who works at the Stanford Research Center, says that we are creating new generations of computer criminals by encouraging our university students to play with computers and teaching them that it's a game. The games turn serious when the students get out in the business world and probe security measures designed to protect personal information or comapny secrets stored in the computers. Susan Nycum, a San Francisco attorney who specializes in computer abuse, states that there is a feeling that anything the person can get hold of i.e. the programs, the computer time, etc., belongs to them. There seems to be no feeling that these things belong to someone else, or that they have any value. In most computer science courses the students are poorly supervised. Students are praised and rewarded for their ingenuity rather than disciplined for various

forms of computer abuse. Most computer science programs at universities do not treat the ethics of computer abuse in a serious manner.

Management must be prepared to deal with the dishonest employee who steals time, currently there is a wide variation of what is considered acceptable. [Ref. 54] Prosecution is nearly impossible for employees who steal company computer time for their own personal projects, time that on a larger computer system is valued at many dollars per second. Few judges understand computer systems, and Florida is the only state with a law specifically making it a crime to steal computer time.

Prior to implementing policies designed to create a secure environment, management must convince each person in the organization that there is a problem, that something can be done about it, and that it is advantageous to do so. For a policy to be effective, it must have a firm commitment by management, complete support by every employee, and it must be supported by trained and competant personnel.

Personnel security problems can range from key-punch and terminal operator errors to destruction of files by mishandling storage media. Ignorance, apathy, and boredom can be as dangerous as intentional dishonesty, but still malicious employees are the most difficult problem for the security manager to cope with. Through carelessness or in anger, an employee can inflict severe damage to computer installations by damaging its program or data libraries. For this reason,

dismissed employees must be denied access to the machine room immediately.

Personnel who have access must be suitably screened so that there is a reasonable expectation of ethical operations. All employees must receive some level of background check to assure their personal integrity. There is a need for evaluation and monitoring of the emotional stability of technical personnel on an on-going basis. Few employees in data processing organizations understand the extent of the trust placed in them and their security responsibilities.

Employees critically engaged in the processing or handling of sensitive or privileged information should be bonded, licensed, and/or certified. In considering the serious problem of employee disaffection: it must be understood that personnel are basically profession oriented rather than company oriented. Oaths of loyalty and nondisclosure should be embedded in contractual agreements for all employees. Employees engaged in the handling or processing of sensitive or privileged information should be familiar with and adhere to established codes of ethics. The assumption must be made that not everyone can be trusted. System security should depend on the integrity of as few people as possible.

The ultimate goal of security and protection of confidentiality is to reduce to a minimum the number of people in whom we must put complete trust and faith. No system of protection can be made absolutely immune to the subversion or deliberate disloyalty of personnel, but if the security procedures are

sufficiently dynamic and sophisticated, the effects of defection, sabotage, and unauthorized disclosure can be minimized. In the final analysis it must be recognized that the integrity of any security program depends on the integrity of the people who have access to the computer room.

VII. SOFTWARE SECURITY

In addition to threats from natural acts, and accidental damage, the data processing manager should spend much of his time preventing the threats via software misuse or unauthorized changes. The most common and the most difficult problem in the computer security business is in the area of software. Stricter security measures are needed badly in software development and application. Software can be copied and sold and the copier is almost guaranteed immunity from any legal action since the original never disappears. Competitors sometimes hire programmers on the hope that even if the programmers will not bring any software with them, they will at least bring all the software ideas. Present computer designs provide for some protection from the accidental losses, yet little or no protection is built in to prevent deliberate attempts to abuse the system by misuse of it's software. Such threats result from an attempt to enter the system so as to molest data or programs, to remove data or programs from the system, to gain free use of the system or to degrade the system in some manner.

Most penetration efforts via software have been completed successfully with about two man-months of effort. [Ref. 48] The bulk of the effort is directed toward finding information to be exploited and building programs to retrieve it. Development of the basic approaches that assure successful penetration has usually required only a man-week or two.

A. SOFTWARE SECURITY WEAKNESSES

In order to understand the problems of providing software security it is necessary to understand some of the hardware and software features of the machine. It becomes quite easy for someone who knows the operating system that controls the flow of programs and data to steal information. A typical time-sharing user only needs to know some of the checks maintained in the operating system to violate the integrity of the system. Since the operating system links the applications program of the users to the hardware of the computer all a user needs to gain access is the password and identity of one of the legitimate users. By expanding his list of passwords he may extend his operating bounds to include all the files of the system. The common term for this abuse is called "masquerading". The threat of masquerading may be minimized by careful handling of passwords, and some care of the selection of passwords. The selection of common names for passwords should be avoided for obvious reasons. The inadequacies of passwords have been noted many times. Passwords simple enough to be easily remembered are usually also easy to compromise. A good practice is to change passwords frequently, but this is rarely done because it is considered inconvenient and unnecessary. However, passwords are the most workable procedure we have now, the latter procedure must be followed if they are to be made a secure procedure.

A clever subverter can get total access to the system by by-passing passwords and taking control of the operating

system. If he can find a fault in the operating system, called "trapdoors", the penetrator is relatively safe from detection. "Trap Doors" are sometimes specially planted entry points by support personnel to obtain data via unauthorized access, and future subversion. Another effective penetration method is called the "Piggy Back" method which involves manipulating messages between the user and the computer, or by cancelling a user's signoff and continuing to operate under his password and authorization.

The "Trojan Horse" class of attack is used in an attempt to achieve the breakdown in security by introducing into the operating system programs with security holes. Imbedding dormant subversive subprograms inside valid programs is typically referred to as a "Trojan Horse" attack. Only a particular condition, such as an alert or activating a special trap door in the operating system will trigger them. This makes it possible for the saboteur to influence the system and its resources even when he is far removed from the situation. If effectively designed this threat could pose a serious threat to tactical weapons systems. For this reason programs and hardware for weapons are exhaustively tested during the development stage. Testing and controlling a weapons system computer is comparatively easier than testing and controlling a general purpose computer because the operating system is smaller, easier to audit, less accessible to outsiders and unauthorized insiders. Data processing managers must establish firm procedures for reviewing and approving "Patches" or program

changes, and access to the object modules must be closely controlled.

The reduction of software failures is a key problem facing computer scientists. It must be expected that programs (of any significant size) will have errors in them. The advent of the loosely defined concept of "structured programming" has done much to make software more reliable. The main underlying concept behind structured programming is to enhance human readability of computer programs. The enhancement of human readability of programs can have a beneficial effect on creating, debugging, and maintaining programs. Structured programming is the construction of entire programs with a series of relatively small modules. Each module should perform a very limited function. The interface between modules are managed by passing parameters. Software reliability, that is reducing the chance of software errors, is enhanced by making modules "suspicious" of the parameters passed to it by other modules. The receiving module can run checks to insure that the parameters received are within valid ranges. While the receiving module cannot insure that the parameter is entirely correct, it can send an error message and avoid improper file maintenance if the parameters are not within proper ranges.

Software dealing with file maintenance can also check the validity of output directed to a file. Once again, the correctness can probably not be verified, but an output outside of a valid range can be prevented. Particularly sensitive object modules should be verified periodically. Assuming that a

standard, approved source program remains available, the source program should be recompiled and the resultant object code put in a file. The new object module and the old object module can then be fed through a text-matching program. The two modules should match; if they don't, the matter should be investigated. Some security is provided by the fact that tampering or alterations with object programs of third generation software is very difficult. If good dicipline is maintained, tampering could only be done by an operator, or an operator in collusion with a systems analyst or programmer.

B. OPERATING SYSTEMS

Security weaknesses, from simple to sophisticated, exist within current operating systems. And the possibility of designing a totally secure software operating system into existing hardware is not realistic and would be extremely costly. Therefore, more reliable program design, acceptance testing and standards is an alternative approach. [Ref. 16] When most operating systems were designed, security was not a primary consideration, and now identification and enumeration of security weaknesses is generally difficult and too expensive. A compromise directed towards providing an acceptable level of security in a current operating system is to add security enhancements to the operating system. However, this is no small problem. Weakness may exist in an operating system because of errors in logic and coding errors. The correction of such a weakness requires checking all interfaces between the user program and the operating system.

In a study conducted by the Government Accounting Office, the following software problems were researched. They are quoted as possible areas of improvement for a more effective control in implementing acceptable privacy/security programs.

1. Adequate communication between the parties to software design.

2. Incorrect perceptions of the nature of actual transactions to be processed.

3. Time constraints hampering the effectiveness of the design process.

4. Absence of written criteria or guidelines for designers to follow.

5. Lack of expertise and experience of programmers.

6. Undetected changes in circumstances making the applications obsolete.

7. State-of-the-art of program testing which prevents testing all possible conditions. Certain solutions have been proposed to assist in the elimination of these sources of error. But mainly one must recognize the completely error-free software cannot be designed; however, the probability of inaccurate documentation can be reduced through implementation of applicable procedures.

C. SOFTWARE SECURITY MEASURES

The following steps should be incorporated into operating procedures to enhance software security:

1. Programmers should not be allowed in the computer room.

2. Operational programs and those under test should be

maintained physically separate.

3. No program should be allowed to operate on live data until documentation is complete and checked.

4. Access to the system must be rigidly controlled and enforced.

5. Each user and process must be isolated from all other programs in the system. Hardware boundry registers, software address traps and various system states should be present.

6. All requests for data access should pass through a system routine which mediates address requests and passes them to the supervisor as a call.

7. Passwords or lockwords should be assignable at least to the file level.

8. Precautions should be taken to prevent the insertion of instructions into programs that might perpetrate a fraud or cause damage.

9. Provide for recovery procedures and restarts.

10. Make sure documentaiton is complete and properly stored.

11. Use file scrambling techniques in real-time systems.

D. CHECKPOINTS AND JOURNALS

Various hardware and software techniques can be used within the system to detect and correct some types of errors before they can adversely effect files. Check sums can be used within hardware to confirm the accuracy of computations or data manipulations. Within the area of data communications, between processors or between terminals and processors, there are various types of codes that can be employed to detect and

correct errors in bits during the transmission (hamming codes or various polynomial codes).

In using checkpoints, the system notes the state of processing at that particular point. The values of certain variables and registers are recorded before proceeding. Should system failure occur after a checkpoint, it is necessary only to restart the processing at the last checkpoint, rather than at the beginning of the entire procedure. Recovery; however, requires one additional factor, a knowledge of what transactions had been processed when the failure occurred. The aforementioned use of checkpoints alone will not, in general, accomplish that.

In batch operations, it is relatively easy to reconstruct all the transactions that were to have been made, but not necessarily those that had already been made. In an on-line environment, the operator may or may not have recorded the entries made at the terminal and may or may not have entered the transactions intended. These problems can be overcome by use of a "journal". Journals can be of varying complexity. The simplest form of a journal records input transactions on a file as they are entered.

E. SOFTWARE PERFORMANCE

The most sophisticated software problem is measuring the conformance of user created application programs to their functional specifications. The vital security question is not whether it does this much, but rather, does it do more than you told the programmer it was supposed to do. Has the

developer of the program, either inadvertently or by design, added to the functional capabilities of the final product features which represent a threat to the integrity of your installation or your data files. /Ref. 48/ The manager often has no recourse but to place the program in service and hope that six months or a year later he does not discover at great expense to his company that the program has all the while been creating a financial nest egg for the programmer. It is an easy task for a programmer to imbed within a legitimate application a self-serving subroutine, or to plant disruptive faults which may be triggered by chance events cognizable by the program, occurring months after he has left the installation or quit the company. What is needed to combat this threat are accountants and auditors who know how to apply their trade to the automatic data processing field.

F. SOFTWARE SECURITY CONTROL SYSTEMS

In addition to the direct elimination of common security weaknesses within an operating system, it may also be feasible to add a security control system. A security control system could be built around partitioning schemes, classifications, run-time assignments and general security rules. The partitioning scheme within the security control system isolates the user from information by both classifications and "permissions". Classifications could be either hierarchical or mutually exclusive. All information within the operating system should be required to have a classification such as confidential, secret, or top secret, Permissions partition

users within the operating system from system functions based on a set of permissions defined for each user. To be fully effective, the control system would have to define classifications and permissions for the user, terminal and the system. The total security control system concept is predicated on individual accountability. The process requires a Security Manager specifying the classifications and permissions authorized for each user.

The security control system requires that all communication end-points (terminals) be known to the operating system. The data processing manager specifies the classifications and permissions authorized for each terminal in the network.

The control system requires that the system environment be defined. That is, the data processing manager specifies the classifications and permissions valid for the system. When the system is defined, any classifications or permissions not included in this definition become unusable for the period of definition.

Thus the assignment of classifications and permissions considers not only those classifications and permissions valid for the user, but those valid for the terminal at which the user is located, and those valid for the system.

The security rules are designed to enforce security within the operating system. The rules must govern access to information, transmission of information, access to a user process, creation of a user process, and access to a system function. For example, a user is granted access to information if the

classification of that information is an element of the user's authorized classifications. A user is allowed to transmit information to a terminal if the classification of that information is an element of the terminal's classification.

G. SUMMARY

A significant part of the total software security problem is adequate definition and control of system documentation. As a result security is improved by limiting each user's knowledge of the system on a need-to-know basis. Some devices for insuring protection include memory protection schemes such as relocation and segmentation, and paging and memory keys which allow limited access i.e. read-only. However, computer architecture is not designed to fully eliminate the ability to obtain access to data through unauthorized methods. The minimum desired protection should be that any attack, successful or not, be detected. A data processing manager's biggest fear should be that a successful or unsuccessful attack may leave no "footprints" or evidence that the system was compromised.

VIII. ELECTROMAGNETIC SECURITY

By far the majority of information collected in government espionage is by interception of data electromagnetically by the use of wire taps, bugs and by monitoring electromagnetic emanations. Techniques, counter-measures and counter-counter measures used in electronic espionage form an expansive professional body of knowledge. Its full coverage is not within the scope of this paper; however, any treatment of data processing security would not be complete without pointing to some of the vulnerabilities from this quarter. Generally, it should be sufficient to state that any information transmitted over commercially leased lines, privately owned point to point lines (switched or unswitched), or over radio waves is subject to interception and exploitation. This threat from interception and exploitation of transmissions and its partial solution is treated at more length in the section on cryptology.

In addition to the interception threat to transmitted data, there are local emanation problems the data processing manager should be aware of for locally processed data. The field strength of electromagnetic emanations increases in proportion to the voltage causing them. Thus low voltage equipment such as a minicomputer's processor will be a less likely source of risky emantions than a visual display unit where deflection potentials of thousands of volts may be encountered. The field strength of electromagnetic emanations likewise increases

in proportion to the current causing them, and for this reason high-current devices such as core memories and electromechanical equipment tend to produce more detectible emanations than low-current devices such as logic circuits.

There are also several unintended conductors in a typical computer room that can absorb emanated power by inductive coupling and radiate it in an undesired manner. Among these are steam pipes; air vents; and raceways, conduit, and cable troughs. If the raceways, conduits, and cable troughs are not already grounded for safety they should be grounded to suppress undesired emanations.

The danger of undesired "accoustical emanations" from the mouths of employees is a great deal more serious than the danger of undesired acoustical emanations from data processing equipment. That is just one important reason for securing against such risks as wiretapping, emanation detection, intrusion devices, and acoustical emanations from equipment; to deprive the culpable employee of any reasonable doubt as to his guilt.

IX. CRYPTOGRAPHY

There are some types of security threats that will resist all the administrative defensive procedures computer users can normally muster. A network user is helpless to prevent a snooper from recording or listening in on his data transmissions. A user may find it inconvenient to lock up disk packs, tape reels, and other removable media containing valuable or sensitive information. To protect against such threats it becomes essential to employ cryptography, which may not only be the best solution to protecting data in transit, but may also be the most cost-effective way to protect stored data as well. While cryptography is the study of methods to protect data from unauthorized viewing, cryptanalysis is the technique used to penetrate encrypted communications and data. [Ref. 23] The basic challenge in cryptography is to devise an encryption algorithm that will withstand intense cryptanalytic efforts.

Cryptographic devices have been effectively used for decades to automatically encode and decode data on communications channels. The techniques used have been highly classified by governments and until recently have seen little use in a commercial environment. For communication channels, crytographic techniques are the only known practical method to prevent access to data from radiation interception or wire tapping. With the expanding use of distributed processing in computer systems; the classical techniques of personnel security and

physical security must be augmented by communication security: the protection of the privacy of information while in transmission. Central to communication security is cryptology which is the transformation of data into a form which is useless to anyone except the intended recipients. The computer security field is becoming more sophisticated technically, and the problem is growing. A big part of the problem is the security of data in transit. With data encryption being the obvious answer to this portion of the problem, $100 million dollar-a-year markets are forecast for data encryption equipment by the 1980's.

The very nature of computerized information systems actually facilitates its unlawful reproduction and transmission to anyone with the tools and know-how. But information stored with scrambling techniques requires sophisticated technology and complex deciphering systems before decoding can even begin. Without the proper key unauthorized use is inexpedient and costly, and the price is raised beyond any reasonable economical effort to exploit it. Thus a high degree of secrecy at minimum cost can be achieved through the use of cryptographic techniques for the protection of sensitive information. While not foolproof, data encryption can be an effective means of denying an intruder any benefits from his ill-gotten gains. Cryptographic techniques can provide an economical method to increase the security of a system beyond the ability of all except the most determined enemy with unlimited resources.

Encryption techniques have been studied for a great many

years, and much effort has been directed toward development of sophisticated encryption algorithms. Traditional cryptographic techniques were developed long before the computer was even thought of, and most of these early techniques are not well suited to computer operations.

Basically, there are two principal classes of cryptography, transposition and substitution. /Ref. 22/ A transporation cipher leaves the letters of the plaintext message unchanged, but the order is rearranged so that the message meaning is concealed within the cipher. In substitution cipher the elements of the plaintext message keep their relative position, but they are replaced in the cipher text by other letters or symbols. There are many variations of both transposition and substitution techniques. Probably the most famous transposition technique was the rail system developed and used during the Civil War. Using the rail system a line of text is split among multiple parallel lines in various orders as if the successive lines were on a rail fence, hence the name rail transposition. The two subclasses of substitution are monalphabetic and polyalphabetic. In monalphabetic methods one letter is substituted for another; it follows that polyalphabetic systems, where more than one letter is substituted, are a bit more difficult to break.

By the fifteenth century an Italian by the name of Alberti discovered a technique to break into messages enciphered by both transposition and substitution. /Ref. 53/ The method was frequency distribution analysis. Once the language was

known, it was simply a matter of using known frequency distributions of letters to derive the hidden plain from the cipher. In 1883 Auguste Kerchkoff established the principle that "the enemy should be assumed to know the encoding technique". The problem is to conceal the key to the algorithm making it of sufficient complexity that an intruder will not be able to determine the key. /Ref. 43/ The cat and mouse games between senders of messages and unintended recipients has continued, and increased with complexity.

A cryptographic method developed in 1917 lends itself well to use in telecommunications and computers. Gilbert S. Vernam, an engineer at AT&T devised a means, using the Baudot code to add a plaintext character to a key character and produce an enciphered character. /Ref. 13/ For example:

Plaintext	11001
Key	10011
Cipher	01010

To derive the text from the cipher, simply add the key to the cipher, i.e.

Key	10011
Cipher	01010
Plain	11001

The use of this method with key tape loops and random key generator machines was the beginning of the modern era of cryptology. Gradually, electronic enciphering systems replaced the mechanical methods. The rapid spread of digital logic has offered many new opportunities to modern crypto

designers. Modern high speed digital computers are prime application candidates for cryptography, and some new microprocessors are already designed as encryption devices. The repetitive nature of most computer files would be too vulnerable to cryptanaletic attack if they were encrypted by low-level techniques; however, even that would still be providing some protection against the casual snooper. One can conceive of ultimate solutions using end-to-end encryption with key generation and forwarding performed automatically by a computer assigned to the task. It will be several years before such schemes can be considered a reality in the commercial world, but much progress has already been made in that direction in military telecommunications.

There are three approaches to incorporating encryption into data communications systems; link-by-link, node-by-node, and end-to-end. [Ref. 47] Link-by-link encryption protects data between directly communicating nodes. This approach avoids having to integrate the cryptographic algorithm into the communication nodes. It can be implemented by using a pair of cryptographic devices to bracket the line between the two nodes. Node-by-node encryption is similar to link-by-link encryption, except that the encryption algorithm is integrated into software modules or peripheral devices attached to the nodes. Each link is still protected by a different key. End-to-end encryption protects messages continuously with the same key until they arrive at their final destination, no decryption is performed at any intermediate node. The cryptographic

algorithm is integrated into the end nodes, i.e. the CPU or the front-end-processor. End-to-end encryption appears to be the most attractive solution for systems having many lines to protect. Only a node that originates encrypted messages or is the final destination for encrypted messages requires cryptographic capability. End-to-end encryption affords greater security than the other two because it allows messages to remain encrypted until reaching their final destination. Link encryption is probably the method most users will elect to use in their first encryption applications. This is because it will be the method which has the minimum impact on hardware and software in existing systems. If dedicated lines are used, which is the perferred way, there should be a different key for each link, and possibly a different key for each direction of traffic on the same link. Link encryption is adequate for protecting against wiretapping but in a network it does not guard against misrouting.

Encryption has been extremely successful in preserving the security of radio teletype message traffic; however, some problems need to be solved before it can be applied on a wide scale to data in computers. [Ref. 48] One of the major questions to be solved is in which parts of a computer system can encryption and decryption be performed. Basically, the other two questions are what protection improvements will encryption provide and what are its limitations? What is the cost/performance penalty to be paid for the introduction of encryption techniques?

Encryption can also be extended to providing protection of data in main storage. For this it will be necessary to put an encryption device between the central processor unit and main storage. It will also be necessary to find a means of handling control information for input and output devices. The channel programs and data for transfer to unit records can be left in decoded form in main storage. This means that the encryption device will have to be turned on and off under program control. Additional encryption devices can be added to the input and output controllers to decode the channel programs and data when necessary. The encryption device can also be placed in the main storage unit. Keys and control information would be sent from the central processor unit and input and output controller at the same time addresses are sent. Several keys will have to be kept in central processor unit registers assoicated with registers containing addresses such as the instruction counter or base registers. These keys must be loaded and unloaded when the corresponding address registers are changed. It will be necessary to have tables of keys in main storage, and these tables will have to be protected, for this we may not be able to rely on encryption. A base/bounds protection mechanism, or a lock and key protection mechanism will probably be necessary.

The most obvious way of providing encryption on a tape or disk is to install an encryption device on each tape or disk drive in line with the data path to the recording head. With everything on the tape or disk in code, the tape or disk

is protected in case it is stolen, and it is easier to dispose of when it is not needed any longer. This configuration has the disadvantage that a large number of encryption devices are required. The number of encryption devices can be reduced by placing the encryption devices in the peripheral control units instead of in each tape or disk drive. For this configuration the encryption device must be designed to be set, enabled, or disabled by the peripheral control unit. This permits encoding of data which is to be recorded by a peripheral device, while not encoding peripheral control and status information.

A very complicated scheme is necessary when files are shared on a need-to-know basis. Data is divided up according to category of information. Each category is assigned to a different encryption key. Each user is provided with a list of keys, the keys corresponding to the data he has permission to access. Transfers should not be encrypted for devices cleared for the same level of classifications.

If scrambling techniques are to be successfully used for computers, repetition of the cryptographic keys must be avoided. The best key system would use a unique key for each record, and in order to protect files from professional code breakers, it will be necessary to change all keys periodically. When this is done all files may have to be copied and recorded using the new keys. This problem could become enormous using installed technology. Hopefully, large scale intergration techniques will solve this encryption problem of stored data.

We are currently limited by a lack of better, faster encryption techniques and speedier, less costly circuits. The main problems to be solved are mainly problems of getting more out of encryption schemes and devices. A major problem will be providing master and submaster key capability for distributing need-to-know level information from multi-encoded files. In most cases, it will be impossible to accomplish encryption of stored data by seting keys manually. It is estimated that 10 million bits per second encryption devices can be built for tape and disk applications, but still faster devices are needed for use between CPU and mainstorage. This too will probably be accomplished through the continuing development of large scale integration.

The cost penalty can become excessive for the introduction of encryption into already existing systems. Here encryption by itself is not enough to protect a system, but must become part of a security plan, and this could have best been accomplished at the initial design of the system. Dispite the difficulties in both the design and use of computational type cryptographic devices needed for computer application, a number of companies have already announced cryptographic devices for commercial use. The two leading venders are IBM and Motorola. The two devices designed by IBM for commercial use are the 3845 and the 3846. /Ref. 29/

Encryption by itself will not be sufficient to protect a system, to be effective it must be interfaced with a variety of other technologies, including physical security, personnel

security, and electronic shielding protection measures. Cryptographic techniques are not a panacea for file security. For cryptographic techniques are of no value if other basic protections are ignored, i.e. if physical security is lax, the thief will simply steal the key. Additionally, there is only one kind of algorithm that you can prove mathematically to be unbreakable, the one time pad. [Ref. 29] This type of cipher is a method where the key is used once and discarded. Even with this algorithm it must be assumed that both the sender and receiver are trustworthy and adhere to proper procedures.

X. MANAGEMENT AND SECURITY

The management of a data processing installation must be in a position of demonstrating to more senior management that is has been responsible in protecting resources entrusted to it. There is a direct conflict in goals between increased accessibility and good security. Traditionally, security was achieved by strictly limiting access to data physically. Along with growing complexity in the computer systems, management needs to formalize their methodology for conducting the basic functions of analysis, planning, and implementing security measures. Much of the methodology exists in the current literature, but not in a connected, comprehensive manner. Non-the-less, the responsibility for initiating computer security lies with the manager of the facility. [Ref. 2] Management should keep in mind that an organization with a sound security program is usually an efficient performing organization, and an organization with a poor security profile is usually inefficient, untidy and may have morale problems.

In dealing with the computer security crisis top policy makers are faced with a growing complexity of desires which translate into conflicting needs and concerns. [Ref. 25] Various committees have often pointed toward a basic destination, but the course has yet to be charted. Current policies and laws are too diverse and unfocused, they are neither coordinated nor comprehensive. In spite of this, management has

recognized computer security as an area of concern, and the dash is on to provide a viable computer security program. There are four basic actions any prospective data processing manager should contemplate when planning a security program.

1. Plan for networks; they are the wave of the future.

2. Write security into the specifications and initial design.

3. Install controls in systems from the beginning.

4. Continually assess and audit those controls.

If these actions are accomplished, the goal of simple, isolatable, measurable and flexible security controls will be very much a current possibility.

The Honeywell Corporation recommends and advises computer users to include the following steps into their systems to improve security:

1. Involve the executives and managers before new systems are implemented. Knowledge of the system by all concerned minimizes the risks and missuse. In the past there has been insufficient management participation in design, development, and implementation of new information systems.

2. Assign a system security officer responsible for looking at the system's security. He can be a full time or part time security officer depending on the size of the operation.

3. Prosecute all known criminals and abusers of the system.

4. Remove all suspects from sensitive positions as soon as they become a suspect.

5. Enforce the law and administrative regulations of the organization.

6. Do not overlook minor infractions of security. Always take positive action to prevent and eliminate reoccurrences.

7. Organize a cooperative system security effort that involves all concerned.

In many cases an outside concultant can do more to educate management as to the impact of risks and potential failure of a computer system and provide normally expected support in solving some of the security problems. There is one other pole that needs to be performed, and which can best be performed by the outside management consultant. That is the role of the system security auditor. To protect the organization against the compromise of its assets, management should turn to a knowledgeable outsider for objectively appraising and testing the adequacy of compliance with security procedures and contingency plans. Realistically, managment must be aware that neither resources nor ingenuity expended for protection can completely protect against all possible threats, but in most cases, the costs of unauthorized penetration can be made to exceed the value of the information obtained.

A. THE COMPUTER SECURITY MANAGER

A new profession, envolved in computer security is developing in automatic data processing. The security problems that this position has responsibility of solving are relatively new to most businesses. One of the first responsibilities of the computer security manager is to define objectives and priority

areas requiring attention. /Ref. 54/

Specific responsibilities of the security officer in charge of data processing security might include the following:

1. Recommendations for purchase, testing and maintenance of fire-resistant cabinets, fire detection and extinguishing equipment, alarms, etc.

2. Develops written contingency plans for various emergencies and conducts related drills.

3. Reviews software standards from a security point of view.

4. Advises higher management of security procedures.

5. Monitors adherence to security procedures.

6. Arranges off-site storage of back-up files and programs.

7. Arranges for back-up computer facilities and conducts trial runs to insure capatability.

8. Advises on the purchase of insurance, and advises the legal department against the insurance company when claims arise.

9. Provide special training for people who need it, such as auditors and physical security guards and officers.

Not only do good security practices reduce the possibilities of loss due to natural disasters and fraud, but insurance companies are usually prepared to offer preferential terms to organizations with realistic and effective security procedures.

The new security manager should look at existing controls

and procedures and rectify any errors or update such policies that require revision. He must evaluate the level of security needed to minimize the potential risk outlined in the plan. He must realize the primary objective is to assist higher management evaluate security problems and implement necessary security standards. The following steps are suggested for developing a comprehensive security program:

1. Identify what needs to be protected.

2. List threats that are likely to occur at your computer facility.

3. Perform a risk analysis.

4. Use the analysis in security planning to justify needed security measures.

5. Develop contingency plans for high risk areas.

6. Repeat this process periodically and analyze trends.

The security manager should remember that security is a line responsibility and line management is accountable for the protection of assets in their custody or under their control. So, to convince management to underwrite security projects or programs, educate them so they develop an awareness of magnitude and complexity of the problems and place the responsibility where it belongs.

XI. RISK ANALYSIS

Risk analysis involves the examination of each possible undesirable situation and a determination of the possible dollar impact of each situation. The objective is to arrive at a statement of risk in cost per unit time, such as dollars per year. This will be matched against the security budget to see how much will be spent on which vulnerability. Risk analysis which can be used as a justification for security plans for any particular environment has received a lot of attention recently. The General Accounting Office has recommended the establishment of "risk management" techniques within the federal government. [Ref. 16]

Unlike the typical risk situation where the value of the potential loss is usually obvious, the loss potential associated with a computer system can only be determined through a systematic and comprehensive quantitative assessment of the risk. The level of risk is acceptable when the frequency with which it occurs times the loss per frequency is so small as to be considered not meaningful to the overall operation.

In performing risk analysis, it is important to note the value of the contents of the typical office will be in the range of $10 per square foot, the same value for a computer room might be as high as $2,000 per square foot. Therefore, security measures should not only focus on the areas of greatest need but consider value disparity of assets. It is most

important to be able to identify the risk in relation to the probability of it occurring. Risk analysis can also determine your company's exposure from down-times. Once the potential losses are known, intelligent decisions can be made regarding the expenditures the organization is willing to tolerate in preparing to avoid down-time.

The first step that must always be taken is to determine a complete list of threat types. /Ref. 48/ The second step involves determining probabilities that these threats will occur. If we list in decreasing probability things that cause loss or damage to data or data systems we would find at the top of the list errors and ommissions. Second would be dishonest employees, and third is fire. Fourth on the priority list is disgruntled employees. Fifth is water damage and finally in last place and accounting for a very small percentage of the losses is loss due to "other causes". This includes penetration of the data systems by strangers. To formulate the most effective security program it is necessary to avoid the human tendency to consider things which might happen but which have a low probability of occurrence. There will also be a natural tendency to avoid any precaution that might impose considerable cost or inconvenience on the data processing facility. It is natural to imagine a much wider array of malicious activities which one can reasonably anticipate happening. Concerns should be reserved for those things which happen with a sufficiently high probability to justify corrective measures including, where appropriate, recovery rather than avoidance.

After the analyst enters the threat probability and cost estimates, calculations of the expected annual dollar losses are made. This is done by multiplying the dollar loss for each threat times either the probability of occurrence, or the annual expected occurrences, which ever is appropriate for that threat. These calculations generate both high and low expected annual dollar losses for each threat. When totaled over all threats, the results provide the best case and worst case yearly forecast of dollar losses to the company.

One does not have to be a graduate statistician or accountant to prepare a risk analysis. The process of obtaining the data and performing the simple calculations is no more complex than other management decision processes. The result of a risk analysis is a table of numbers which identify; threats, cost of threat occurrence, probability of occurrence and finally the expected dollar cost to the company.

An example of how to do a risk analysis is presented in Table I which shows four major hazard areas: computer facility, hardware, software, and personnel. /Ref. 16/ For each area the significant system threats are listed, and each threat has been evaluated in terms of the minimum/maximum dollar losses to the company. The analysis provides a probability of occurence for each threat.

Much of the probability data needed can be obtained from outside sources. Many federal, state, and local agencies can provide the probability that natural disasters will occur in a given year. Insurance companies can provide statistics on

TABLE I

SAMPLE RISK ANALYSIS

THREAT	(000) RANGE OF $ LOSSES PER OCCURRENCE MIN	MAX	% PROBABILITY OF AN OCCURRENCE	EXPECTED ANNUAL OCCURRENCES	EXPECTED ANNUAL DOLLAR LOSS LOW	HIGH
1. Computer Facility Hazards						
Natural Disasters						
Earthquake	10 -	3,000	0.1		$ 10	$3,000
Windstorm	2 -	400	0.4		8	1,600
Flood	1 -	100	0.1		1	100
Lightning	1 -	50	0.1		1	50
Rain & Mud	2 -	50	0.9		18	450
Ice & Snow	1 -	10	0.1		1	10
Physical Hazards						
Fire	10 -	3,000	0.6		60	18,000
Loss of Utilities	2 -	200	5.0		100	10,000
Air Conditioning Failure	5 -	100	2.0		100	2,000
Communications Loss	1 -	300	12.0		120	36,000
Explosions	10 -	100	0.1		10	1,000
Water Damage	5 -	500	0.3		15	1,500
Industrial Accident	20 -	500	3.0		600	15,000
2. Losses Caused By Hardware						
Central Processor	1 -	10		3	3,000	30,000
Peripheral Units	0 -	1		20	0	20,000
Communication Processor	0.1 -	3		5	500	15,000
Graphics Equipment	0.1 -	.5		8	800	4,000
Terminals	0 -	.1		20	0	2,000
Data Collection Hardware	1 -	3		4	4,000	12,000
3. Losses Caused By Software Failure						
Operatin System	1 -	10		1	1,000	10,000
Compilers,Editors,Utilities	5 -	10		2	10,000	20,000
Application Software	0.1 -	.8		20	2,000	16,000
Data Files	5 -	10		3	15,000	30,000
4. Losses Caused By Human Failure						
Errors and Oversights						
Programmers	0.3 -	2		10	3,000	20,000
Operators	0.1 -	0.3		25	2,500	7,500
Production Setup	0.1 -	0.3		5	500	1,500
Maintenance	0.1 -	0.5		2	200	1,000
Data Entry Operators	0.1 -	0.2		30	3,000	6,000

TABLE I (continued)

Computer Abuse				
Vandalism	1 - 10	2	2,000	20,000
Espionage	1 - 20	1	2,000	20,000
Fraud	1 - 4	5	5,000	20,000
Theft	1 - 5	6	600	30,000

BEST CASE FORECAST	$55,154	
WORST CASE FORECAST		$373,260

the probability of fires, and industrial accidents. Other outside sources are computer vendors, universities, and law enforcement agencies. Already much data regarding the probability of occurrence of computer security problems has been published in books and security journals. Donn Parker at the Stanford Research Institute also collects records of security threats. Based on his data, prior probability estimates and cost estimates for many security threats will become easier to establish.

Some key questions you might want to consider when performing a risk analysis are:

1. Which of your data processing assets are the most valuable to you?

2. How valuable are they? Or what would the effect be on your organization if they suddenly were not there?

3. What hazards threaten each of these assets?

4. How do you select protective measures? Or how much should be spent to protect the assets?

5. How can you determine the residual risk once a number of protective measures have been implemented?

The analyst will soon realize that it is not possible to provide absolutely accurate probabilities and costs, and because of this, many worry about the usefulness of risk analysis. Quantification of risks and costs is a process of estimation, always involving inaccuracies, and is no different than any other fact finding process. But even using data based on an estimation process, risk analysis provides a means of ordering

the relative importance of various threats. This gives management better perspective of the overall situation, and it certainly better than doing nothing at all. Frequently, the key to success lies in the ability to recognize and quantify the elements of risk so that we are able to deal with them in an objective way.

A risk analysis provides an approach managers can easily implement and use. By systematically applying the risk analysis approach, managers of data processing centers can gain a better understanding of their total security picture: vulnerabilities, costs, and trends. With this better understanding, managers can initiate actions to reduce the costs and risk associated with the company's computer investment, and thus fulfill one of their major responsibilities. Finally, risk analysis encourages managers to establish policies which require the orderly recording of problem and failure data. Risk analysis does not have to be expensive, and if diligently applied can provide substantial benefits to the organization.

XII. DATA PROCESSING AUDITING

Basically, data processing auditing is evaluating security measures, identifying areas of exposure and recommending corrective actions. The creation of an audition process by which the adequacy of procedures and compliance to procedures are routinely assessed is a large task. However, data processing auditing could provide immediate warnings of illegal system penetration. Qualified data processing auditors who are independent of designers and users should review the system design prior to coding and testing. A review of the operation of these applications should also be conducted shortly after implementation.

It is significant that most cases of computer abuse have been discovered by accident rather than through purposeful methods. [Ref. 48] Currently, there is no unifying audit techniques or technology beyond dealing with the most rudimentary batch-oriented systems. Yet much computer abuse could be avoided with even simple, rudimentary attention to audit details such as internal controls for validity checks, error handling procedures, control totals, accounting for computer time and spot verification of computer output. For these reasons, the internal auditor needs to play a larger role in the data processing part of the agency or business. There is a lack of awareness among auditors to the vulnerabilities of data in computers. There is a definite need to develop and

document practices and procedures for auditors in data processing environments.

Auditors should ensure that the simple, inexpensive, but effective security measures are taken before they worry about more elaborate measures to protect other, but equally vulnerable situations. The estimated loss expectancy discussed in the previous chapter, provides a gauge for determining a reasonable level of expenditure for protective measures. The security audit program should draw on the risk analysis to identify the areas which require the most attention.

The role of the auditor is vitally important to the security of the system. He should work with the data security manager to spot check and subject the system to accuracy and validity checks. Auditors must be trained to recognize creative fraud, and new fraud activities from both inside and outside the organization.

Upon concluding an audit, the auditor signs his name to a statement which says in affect, this system is secure within the bounds established in the design concept and determined by the risk assessment.

XIII. INSURANCE

Even though the computer has been in the mainstream of business for two decades, some types of data processing insurance are not routine. Insurance companies are generally inexperienced with data processing insurance. They are reluctant to insure remote terminals, communications cost or switch gear mainly because they do not understand the technicalities involved.

Most insurance underwriters never heard of a data base online files which might require several hundred thousand dollars to rebuild and rebalance. Insurance companies consider data processing insurance by itself a bad business venture. They prefer to include data processing as part of a total business package. When you do find an insurance company that does write data processing insurance, most likely he will negotiate totally with the comptroller for a "blanket policy" and may not even talk to the data processing manager. Despite this, the situation is improving and currently there are several types of data processing insurance currently available in the form of negotiated agreements. The most popular types are:

1. Equipment and facilities
2. Loss due to business interruption
3. Storage media and its contents
4. Extra expense at a backup site
5. Delay in collecting accounts receivables
6. Valuable papers and records

7. Malpractice, including human errors and omissions

When the data processing manager is not consulted, and the coverage is negotiated by the comptroller and the insurance company, the data processing manager must not assume he is properly covered. To assure himself of adequate data processing coverage, he should enumerate all files and estimate the labor and machine time required to reconstruct each of the files, and then total up the replacement costs of the data processing library. Estimates should include the extra expense likely to be incurred for temporary facilities, machine rental, overtime on the staff, couriers, etc., so it will be possible to continue to operate until the move back to the regular facility. If the operation includes extensive timesharing or other on-line services, communications costs become very important. Make sure the extra expense checklist includes telecommunications expenses or there could be a three-way argument later between the data processing manager, the comptroller, and the insurance company.

Idealistically, a good manager should manage his risks down to some reasonable level and then insure himself against the residual. Once the decision is made to insure against exposures, then it will be necessary to place a dollar value to each exposure, and declare that value to the insurance agent, and pay a percentage of that declaration as a premium for proper coverage.

Some risk situations are essentially uninsurable because the magnitude of the risk cannot be assessed. For instance, it would be impossible to assess the value of certain medical

records, undiscolsed inventions, or military secrets. Insurance against inadvertent disclosure, data processing errors, or the acts of malicious employees is difficult to get, and so expensive that when faced with the premiums most data processing managers would search for ideas to reduce risks using good security or better procedures.

In summary, enumerate your risks, quantify them, and discuss a course of risk management with the comptroller annually. Whenever there is a substantial change in hardware, software, application or on-line services, estimate how this changes the insurance risk and promptly inform the comptroller in writing. Be sure to estimate the number of days of likely operation in a backup facility in case of a catastrophe. Be aware that, in some cases, a catastrophe would signal an immediate equipment upgrade. In such a case, insure the insurance covers depreciated value plus the costs of a crash reprogramming job, changes to the affected external procedures, and training of personnel.

XIV. CONCLUDING REMARKS

Computers are becoming more and more important in the running of large organizations, costs are going down, and use is expanding almost exponentially. This has combined to create a computer security problem of enormous proportions and it is now essential for computer installations to have a computer security program. For any security program to succeed, it must have management involvement from the top down. The program should be implemented and maintained under the direction of a security administrator.

There is no excuse for management failure to respect the value of data entrusted to their care by taking necessary steps to ensure its protection. Each organization must be considered unique and management must design a security program tailored to its own particular requirements. All the preventions and all the protection in the world will not stop computer crimes or abuses. However, leaders and managers who are aware of the existence of crime can be alert to its occurrence and may be able to detect it in the early stages to reduce its devastating effects.

Develop an education and training program aimed at promoting security awareness with all data processing associated personnel. Ensure that the installation is checked for electromagnetic emanations and listening devices (bugs) at least annually. If at all possible, encrypt any form of communications which leaves

the computer center. Important documents should be sent via registered or guard mail. Using these approaches, one can begin to formulate an acceptable defensive threshold. The procedures adopted by the installation must avoid making it easy to violate good practice. Systems security monitoring and surveillance of the computer organization is necessary to ensure that the integrity of the existing policies and procedures have not deteriorated. The security manager should be aware that a determined perpetrator loves to deal with the checklist mentality, and everything done to stop him is written down. If he can get a copy of the security plan, it would give him an almost infinite set of possibilities to choose from in carrying out his scheme.

Efforts to solve computer security problems are beginning to match the importance of this weakness with the data processing field. However, we are just now beginning to enter the productive stage in solving the basic problem. AT&T is currently trying to improve telephone security which may even lead to customer tariffs on security services. [Ref. 29] Eventually, AT&T may even use public key cryptography to provide a completely secure phone system. Privacy regulations and pressure from federal agencies and insurance companies will give impetus to this trend. Encryption will be used initially to protect sensitive data during transmission and will be increasingly applied to some aspects of data storage. Within federal, state and local governments, data encryption will become mandatory to protect the confidentiality of sensitive data bases.

Much effort has been expended in attempts to solve security problems by retrofitting security modules on data processing systems already in operation. After millions of dollars worth of research and too many manhours of effort, it has been proven repeatedly that retrofitting, while providing more security than before, is still subject to penetration by a sharp computer oriented individual or group. An infiltration attempt by a team from the Rand Corporation against a supposedly very secure system accomplished the following:

1. Listed the contents of a security protected pseudofile at a remote terminal.

2. Circumvented the access protection mechanism and processed the file directly.

3. Listed the security protected password at a remote terminal.

4. Inserted a "trapdoor" for future circumvention.

5. Accomplished all the above undetected.

It is now accepted that the best way to attack the computer security problem is to design a system of integrated hardware/software from the ground up. The development of secure systems will necessitate balancing the many tradeoffs; systems architecture, hardware design, software design, operational constraints, and initial cost and ongoing operating costs. The nature of the problem necessitates careful and objective selection from among the many alternative solutions that are available. The problem is sufficiently complex so as to require inputs from personnel with expertise in systems

architecture, programming, cryptography, psychology, accounting, and other specialties. An effective security system must include the total environment: physical and procedural safeguards as well as those provided by hardware and software.

Security is not a clearly defined, carefully delineated, quantifiable objective. It is an assessment of risk, which involves not only the interplay of hardware and software, but also physical and administrative controls and a good deal of awareness on the part of people working with computers.

How much security is needed must be based on cost benefit analysis. The extent of security measures depends on the assets to be protected and the perceived risk. Management must remain aware that no system of security is 100% secure, if a perpetrator has enough time, resources, and determination, any system can be broken. What the DP manager must do is to raise the "price" of breaking into the system so it is no longer worth the perpetrator's effort. The overall data security plan must be a three-pronged attack on the problem:

1. Minimize the probability of a security incident occurring.
2. Minimize the damage caused by a security incident.
3. Enhance the recovery from the effects of a security incident.

Finally, to paraphrase a famous saying: "eternal vigilance is the price of data security".

LIST OF REFERENCES

1. Anderson, R. A., and Kumpf, W. A., Business Law, Principles and Cases, Sixth Edition UCC, South-Western Publishing Company, 1975.

2. Becker, R. S., The Data Processing Security Game, Pergaman Press, 1977.

3. Beizer, B., The Architecture and Engineering of Digital Computer Complexes, Volume 2, Plenum Press, 1971.

4. Carroll, J. M., Computer Security, Security World Publishing Co. Inc., 1977.

5. Coquis Rondon, E. E., Digital Encoding For Secure Data Communications, Thesis Electrical Engineer, Naval Postgraduate School, 1976.

6. DoD 5200.28, Security Requirements for Automatic Data Processing (ADP) Systems, 18 December 1972.

7. DoD 5200.28-M, ADP Security Manual of January 1973.

8. Dragunas, D. J., Security in Computer Systems, Computers in the Navy, The Naval Institute Press, 1976.

9. Enslow, P. H. Jr., What is a Distributed Processing System, Computer, Volume 11, Number 1, January 1978.

10. Gammon, H. M., and Hattery, L. H., Managing the Impact of Computers in the Federal Government, the need for Central Planning, The Bureaucrat, Volume 7, Number 2, Summer 1978.

11. Good, George E., New Developments in Data and Voice Security, Telecommunications, Vol. 8, No. 3, March 1974.

12. Gottlieb, C. C., and Borodin, A., Social Issues in Computing, academic Press, 1973.

13. Greenlee, B. M., and Jacobson, R. V., Computer and Software Security, AMR International, Inc., Advanced Management Research 1972.

14. Heinrich, F. R. and Kaufman, D. J., A Centralized Approach to Computer Network Security, AFIPS Conference Proceedings, Vol. 45, AFIPS Press, 1976.

15. Hoffman, L. J., Modern Methods for Computer Security and Privacy, Prentice-Hall, Inc., 1977.

16. Honeywell Information Systems, Proceedings of 3rd National, Computer Security and Privacy Symposium, April, 1977.

17. Hurley, Mark J., The Privacy Crisis, Catholic Information Service, No. 73.

18. Jancura, E. G., Audit and Control of Computer Systems, Petrocelli/Charter, 1974.

19. Jancura, E. G., Computers Auditing and Control, Petrocelli/Charter, 1977.

20. Janssens, C. J., Privacy Legislation and Its Implication Toward the Computer Industry, M.S. Computer Science, Naval Postgraduate School, 1977.

21. Jolly, J. A., Creighton, J. W., Moore, B. M., Technology Transfer in Science, Technology and Public Policy, Naval Postgraduate School, 1978.

22. Katzan, H. Jr., Computer Data Security, Van Nostrand Reinhold Compnay, 1973.

23. Kahn, D., The Codebreakers, MacMillan, 1967.

24. Larson, D. L., Computer Data Security, M.S. Thesis Computer Science, Naval Postgraduate School, 1974.

25. Lee, T., Why the Nation Sorely Needs An 'Information Constitution', Government Executive, November 1978.

26. Lupton, W. L., A Study of Computer Based Data Security Techniques, M.S. Thesis Computer Science, Naval Postgraduate School, 1973.

27. Mair, W. C., Wood, D. R. and Davis, K. W., Computer Control and Audit, The Institute of Internal Auditors, Inc., 1978.

28. Martin, J., Security, Accuracy and Privacy in Computer Systems, Prentice-Hall, Inc., 1973.

29. Meyer, C. H., and Tuchman, W. L., Putting Data Encryption to Work, Mini-Micro Systems, October 1978.

30. Myers, G. J., Software Reliability, Principles and Practices, John Wiley and Sons, 1976.

31. National Bureau of Standards Special Publications 500-21. Vol. 1, Design Alternatives for Computer Network Security, Cole, G. D., U.S. Government Printing Office, 1978.

32. National Bureau of Standards Special Publication 500-21, Volume 2, The Network Security Center: A System Level Approach to Computer Network Security, Heinrich, F., U.S. Government Printing Office, 1978.

33. Neat, C. E., A New Computer Cryptography: The Expanded Character Set (ECS) Cipher, Ph.D, dissertation, University of California, Los Angeles, 1975.

34. Office of Telecommunications Policy; Legal Protections of Privacy, Final Report; Creenwalt, K., U.S. Government Printing Office, 1975.

35. OPNAV Instruction 5510.131, Security Requirements for Automatic Data Processing (ADP) Systems, 1 June 1973.

36. Parker, D. B. and others, Computer Abuse, National Technical Information Service, November 1973.

37. Parker, D. B., and Nycom, S., The New Criminal, Datamation, Vol 20, No. 1, January 1974.

38. Prywes, Noah S., "Some Problems and Considerations of Computer Security", Naval Ship Research and Development Center (NSRDC), Proceedings on the Conference on Secure Data Sharing, August, 1973.

39. Reed, I. S., The Application of Information Theory to Privacy in Data Banks, Rand Corporation, 1973.

40. Standford Research Institute, Systems Auditability and Control Study; Data Processes, Audit Practices Report, Ruder, B., Eason, T.S., See, M.E., and Russell, S.H., The Institute of Internal Auditors, Inc., 1977.

41. Stanford Research Institute, System Auditability and Control Study; Data Processing Control Practices Report; Russell, S. H., Eason, T. S., and Fitzgerald, J. M., The Institute of Internal Auditors, Inc., 1977.

42. Suess, K. M., Computers, Privacy and the American Public, Technology Transfer in Science, Technology and Public Policy, Naval Postgraduate School, Monterey, CA, 1978.

43. Van Tassel, D., Computer Security Management, Prentice-Hall, Inc., 1972.

44. The Ombudsman Committee on Privacy, Los Angeles Chapter, Privacy, Security, and the Information Processing Industry, Association for Computing Machinery, 1976.

45. Toffler, A., Future Shock, Random House, Inc., 1970.

46. Turn, R., A Brief History of Computer Privacy Security Research at Rand, Rand Corporation, 1972.

47. U. S. Department of Commerce, Considerations in the Selection of Security Measures for ADP Systems, U. S. Printing Office, 1978.

48. U. S. Department of Commerce, Privacy and Security in Computer Systems, U. S. Printing Office, 1974.

49. Van Dam, A., and Stankovic, J., Distributed Processing, Computer, Volume 11, Number 1, January 1978.

50. Walker, Bruce J. and Blake, I. F., Computer Security and Protection Structures, Dowden, Hutchingson and Ross, Inc., 1977.

51. Wasserman, J. J., Plugging the Leaks in Computer Security, Harvard Business Review, September-October, 1969.

52. Wasserzug, L. L., EDP Security-Mutual Assistance Agreements, IBM Data Security Symposium, April, 1973.

53. Westing, A., Privacy and Freedom, Atheneum, 1967.

54. Winkler, S., and Danner, L., Data Security in the Computer Communications Environment, Computer, Volume 7, Number 2, February 1974.

55. Wooldridge, Corder, and Johnson, Security Standards for Data Processing, John Wiley and Sons, 1973.

56. Yearsley, R. B., Graham, G.M.R., Handbook of Computer Management, Halsted Press, 1973.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Documentation Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93940	2
3.	Department Chairman, Code 54Js Department of Administrative Sciences Naval Postgraduate School Monterey, California 93940	1
4.	Professor John W. Creighton, Code 54Cf Department of Administrative Sciences Naval Postgraduate School Monterey, California 93940	4
5.	Robert S. McCormack, CDR, USN, Code 52Ms Department of Computer Science Naval Postgraduate School Monterey, California 93940	1
6.	Lieutenant Kenneth Lee Nelms, USN Electronics and Communications Programs Curricular Office (Code 32) Naval Postgraduate School Monterey, California 93940	1